IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

PLANO ENCRYPTION TECHNOLOGIES, LLC, Plaintiff, **v.** **Q2 HOLDINGS, INC. and Q2 SOFTWARE, INC.,** Defendants.	**CIVIL ACTION NO.** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Plano Encryption Technologies, LLC, by and through its attorneys, alleges as follows:

PARTIES

1. Plano Encryption Technologies, LLC ("Plano Encryption") is a limited liability company organized and existing under the laws of the State of Texas, with its principal place of business at 903 18th Street, Suite 224, Plano, Texas 75074.

2. Upon information and belief, Defendants Q2 Holdings, Inc. ("Q2 Holdings") and its wholly owned subsidiary, Q2 Software, Inc., doing business as Q2 ("Q2 Software") (collectively "Defendants" or "Q2" when it is not necessary to distinguish between the two entities), are Delaware corporations, both with their principal place of business at 13785 Research Blvd., Suite 150, Austin, TX 78750.

JURISDICTION AND VENUE

3. This is an action for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code. This Court has jurisdiction over the subject matter of this action under 28 U.S.C. §§ 1331 and 1338(a).

4. Venue is proper in the Eastern District of Texas under 28 U.S.C. §§ 1391(b) and (c) and 1400(b) because Defendants have committed acts and/or contributed to or induced acts of patent infringement within this judicial district giving rise to this action, and Defendants continue to conduct business in this judicial district, including one or more acts of selling, using, offering for sale, licensing and/or distributing infringing products or providing service and support to Defendants' customers in this District.

5. This Court has personal jurisdiction over Defendants for at least the following reasons: (i) Q2 has committed acts of patent infringement and/or contributed to or induced acts of patent infringement by others in this District and this State and continues to do so; (ii) Q2 regularly does business or solicits business, engages in other persistent courses of conduct, and/or derives substantial revenue from products and/or services provided to its customers in this District and in this State; (iii) Q2 has purposefully established substantial, systematic and continuous contacts with this District and expects or should reasonably expect to be subjected to this Court's jurisdiction.

BACKGROUND

6. Plaintiff Plano Encryption is the owner by assignment of United States Patent No. 5,391,399 ("the '399 Patent" or "Patent-In-Suit"), issued November 23, 1999, for "Method for Securely Distributing a Conditional Use Private Key to a Trusted Entity on a Remote System." A true and correct copy of the '399 Patent is attached as Exhibit A.

7. Plano Encryption is the owner of United States Patent No. 5,974,550 ("the '550 Patent") entitled "Method for Securely Authenticating Another Process in a Different Address Space." The '550 Patent issued on October 26, 1999. A true and correct copy of the '550 Patent is attached as Exhibit B.

8. Plano Encryption holds all right, title and interest in the '399 Patent and the '550 Patent (collectively, the "Asserted Patents" or "Patents-in-Suit"), including all rights to bring suit and recover for all past, present and future infringements thereof.

9. The invention of the '399 Patent relates to methods and apparatuses used to secure communications between parties and securely distribute data through the building of software modules including cryptographic keys, that are resistant to tampering. As such, the '399 Patent represents fundamental technology in the field of encryption and secured online data communications. The '399 Patent has been referenced hundreds of times by other patents and patent applications. Nearly every computer company of any prominence has cited the patent more than once during prosecution of their own patents, including leaders in the field of software and computing, such as Microsoft (more than 75 citations), Google (more than 40 citations), and IBM (more than 20 citations). The patent has also been cited as prior art by U.S. Patent Examiners more than 150 times during the prosecution of other patents.

10. The invention of the '550 Patent relates to methods and apparatuses used to secure communications between two processes (a first and a second) running in different address spaces by authenticating a process running in an address space different from another address space thereby allowing for a more secure challenge response protocol.

11. Q2 is in the business of making, selling, offering to sell, licensing and distributing secure, cloud-based, virtual banking software solutions, to regional and community financial institutions, as well as providing customer support, training and implementation services.

12. Q2's mobile banking applications software products and services, including but not limited to its Q2mobility App (the "Accused Products"), allow a customer's retail and commercial account holders to access, engage and complete banking transactions from their mobile or tablet device. *See, e.g.,* "Q2mobility App uses the native functionality of mobile and tablet devices, such as touch, camera and geo-location to enhance the virtual banking experience of account holders." Q2 2015 10-K at p. 10.

13. Q2 actively distributes and promotes its Accused Products for use by its customers' retail and commercial account holders on their Apple iOS or Android-enabled mobile or tablet devices. In doing so, Q2 actively markets and widely touts the importance of the security of its virtual banking solutions. *See* Q2 2015 10-K at p. 5, "The proliferation of mobile and tablet devices and evolving consumer expectations for modern and intuitive user experiences increases the challenges of offering virtual banking solutions… Security is of paramount importance in virtual banking…"

14. On information and belief, Q2 has been aware of the Patents-in-Suit for over one year. Between May and June of 2015, Plaintiff gave notice to various customers of Q2 of Plano Encryption's rights in the Patents-in-Suit, including but not limited to, Independent Bank via letters to Messrs. David R. Brooks (CEO of Independent Bank) and Torry Berntsen (President and COO of Independent Bank), American Bank of Texas, via letters to Messr. B. Wes Shelton (CEO of American Bank of Texas), and Broadway Bank, via letters to James D. Goudge (CEO of Broadway Bank) and Joe C. McKinney (Vice Chairman of Broadway Bank). On information

and belief, Q2 is the provider of the mobile banking applications used by all these banks, and is under an obligation to indemnify these banks for any allegations of patent infringement arising from their use of its Accused Products. On information and belief, Q2 was made aware of the Patents-in-Suit by its customers at least as early as May or June 2015. Thus Q2 has had notice and actual or constructive knowledge of the Patents-in-Suit at least since that time.

15. With knowledge of the Patents-in-Suit, Q2 intentionally makes, sells, offers to sell, licenses and distributes the Accused Products, and provides implementation, maintenance and customer support services related thereto, to its customers including the above mentioned banks in the Eastern District of Texas and many more for use on Android and iOS operating systems as found and used in all Android and iOS smart phones and tablets.

16. On information and belief, Q2 has been, among other things, purposefully, actively, and voluntarily making, selling, offering for sale, using, licensing and/or distributing infringing mobile banking software products and services, including but not limited to its Q2mobility App, with the expectation that they will be distributed, licensed, and/or used by consumers in the Eastern District of Texas. Customized versions of the Accused Products have been and continue to be purchased, used, licensed and distributed by customers and their customers' account holders in the Eastern District of Texas. Q2 has thus committed acts of patent infringement within the State of Texas and in this District and/or has contributed to or induced others to use, license and/or distribute its products and services in an infringing manner, including its customers, who directly infringe the Patents-in-Suit. By purposefully and voluntarily distributing one or more of its infringing products and services, Q2 has injured Plano Encryption and is thus liable to Plano Encryption for infringement of the Patents-in-Suit at issue in this litigation.

17. On information and belief, through its actions Q2 has infringed the Asserted Patents and actively promoted others to infringe the Patents-in-Suit, contributing to or inducing acts of patent infringement by others including its customers, through its use, sale, offer for sale, licensing and distribution of its Accused Products.

18. On information and belief, Q2 has been and now is directly infringing in the State of Texas, within this judicial district, and elsewhere in the United States, by, among other things, making, selling, offering to sell, licensing and distributing its Accused Products, which infringe one or more claims of the Patents-in-Suit, including at least Claim 1 of the '399 Patent and Claim 14 of the '550 Patent. Defendants are thus liable for infringement of the Patents-in-Suit pursuant to 35 U.S.C. § 271. Q2 not only makes, sells, offers to sell, leases, licenses and distributes hosted software solutions practicing these claims, it induces, and or contributorily infringes through the sale, offer for sale, licensing and distribution of software solutions hosted by its customers.

19. Plaintiff Plano Encryption has been and will continue to suffer damages as a result of Defendant's infringing acts.

20. Plaintiff Plano Encryption seeks monetary damages and prejudgment interest for Defendant's past and ongoing infringement of the Patent-in-Suit.

21. The allegations set forth herein with respect to each asserted patent claim, each accused product, and each specific accused feature are exemplary. Plaintiff Plano Encryption reserves the right to assert additional claims, accuse additional products, and accuse additional features.

COUNT ONE

INFRINGEMENT OF U.S. PATENT NO. 5,991,399

22. Plaintiff Plano Encryption realleges and incorporates herein the preceding paragraphs of its Complaint.

23. Defendants have directly infringed and continue to infringe at least claim 1 of the '399 Patent by making, using, testing, selling, licensing, offering for sale within the United States at least the Accused Products.

24. Q2's Accused Products are made available for use through the Apple iOS App Store and the Google Android Play Store. On information and belief, such mobile applications software must be code signed with a private key of an asymmetric key pair, the Q2 Accused Products thus include a private key from a generated asymmetric key pair. The code signing process employs a private key to generate a cryptographic hash that is used to validate the code has not been altered or corrupted since it was signed.

25. Therefore, Q2 (or others under Q2's direction and control) generates at least one asymmetric key pair used to code sign the Accused Products for distribution on these platforms and is generated by the computer used to develop the Accused Products, or Q2 induces or contributes to such generation of key pairs. In the alternative, because the manner of use by Q2 differs in no substantial way from language of the claims, if Q2 is not found to literally infringe, Q2 infringes under the doctrine of equivalents.

26. On information and belief, computers and/or servers that are hosted either by Q2 on behalf of its customers or directly by Q2's customers, interact with Q2'sthe mobile application software once it is downloaded onto a mobile device. *See* Q2 Form 10-Q or Quarterly Report dated May 10, 2016, for the quarterly period ended March 13, 2016, at p. 9, stating Q2 derives "the substantial majority of its revenues from subscription fees for the use of its solutions hosted in the Company's data centers…."

27. On information and belief, at least one other asymmetric key pair is generated either by computers, server(s) or the mobile application software on mobile devices during operation of Q2's mobile application software installed on a mobile device, and Q2 either generates or induces generation of those key pairs. Those key pairs are used to establish secure communications between the mobile application and the server, specifically for SSL/TLS communications.

28. Q2's Accused Products, its mobile applications, use SSL/TLS encryption. As per the TLS protocol, the server and client negotiate the details of which encryption algorithm and cryptographic keys to use. In particular, SSL/TLS uses a handshake with an asymmetric cipher to establish cipher settings and a shared key for a session, while the rest of the communication is encrypted using a symmetric cipher and the session key. The TLS handshake begins when a client connects to a TLS-enabled server requesting a secure connection and presents a list of supported cipher suites (ciphers and hash functions). From this list, the server picks a cipher and hash function that it also supports and notifies the client of the decision. The server then sends back its identification in the form of a digital certificate. The certificate contains the server name, the trusted certificate authority (CA) and the server's public encryption key. To generate the session keys used for the secure connection, the client encrypts predetermined data with the server's public key and sends the result to the server (which only the server should be able to decrypt with its private key); both parties then use this predetermined data to generate a unique session key for subsequent encryption and decryption of data during the session.

29. Data that is determined prior to encryption is encrypted with one or more public keys of an asymmetric key pair. Specifically, the premaster secret data is encrypted with the public key of the key pair generated for the SSL/TLS connection. The client (with the

cooperation of the server, depending on the cipher being used) creates the pre-master secret for the session, encrypts it with the server's public key (obtained from the server's certificate), and then sends the encrypted pre-master secret to the server. This pre-master secret data is predetermined by communications between the server and client. If the server has requested client authentication, the client also signs another piece of data that is unique to this handshake and known by both the client and server. In this case, the client sends both the signed data and the client's own certificate to the server along with the encrypted pre-master secret. If the server has requested client authentication, the server attempts to authenticate the client using an asymmetric public key for verifying the digital signature. If the client cannot be authenticated, the session ends. If the client can be successfully authenticated, the server uses its private key to decrypt the pre-master secret, and then performs a series of steps (which the client also performs, starting from the same pre-master secret) to generate the master secret. In the alternative, because the manner of use by Q2 differs in no substantial way from language of the claims, if Q2 is not found to literally infringe, Q2 infringes under the doctrine of equivalents.

30. On information and belief, Q2's servers and mobile applications build, and/or induce or contribute to other parties building, an executable tamper resistant key module identified for its mobile banking app. When a secure communication of information is requested by a user of the mobile app, the software builds an executable tamper resistant key module. Specifically, the mobile application comprises an executable tamper resitant key module. This key module is identified for a selected program, namely either the iOS or Android set of instructions which is used to create a secure communication in connection with the mobile application. The mobile application includes the generated private key as part of the digital signature process. The mobile application also includes the encrypted predetermined data as part

of the SSL/TLS connection process. The code signing with the private key causes the mobile application to be tamper resistant. This tamper resistant module is used to exchange sensitive information, such as customer account information. In the alternative, because the manner of use by Q2 differs in no substantial way from language of the claims, if Q2 is not found to literally infringe, Q2 infringes under the doctrine of equivalents.

31. Defendants' infringement is and has been willful, deliberate and intentional. On information and belief, Defendants had pre-suit knowledge of the '399 Patent no later than May or June 2015. Q2 has acted and continues to act in disregard of the high likelihood that its actions constitute direct and indirect infringement of a valid patent, and knew or should have known of that objectively high risk.

32. Defendants have knowingly induced and continue to induce users of mobile devices to infringe the '399 Patent, including by intentionally developing, making, marketing, advertising, providing, distributing and licensing the software, documentation, materials, training or support and aiding, abetting, encouraging, promoting or inviting use thereof.

33. Defendants have contributed and continue to contribute to the infringement of the '399 Patent by users of the mobile computing devices, including for example, mobile phones and tablet computers, who use, test, sell, license, offer for sale, distribute and license within the United States, the Accused Products on such devices, by providing the necessary software and related documentation, materials, marketing and advertising, training or support. For example, the above described necessary features of the Accused Products are material components of the patented method as disclosed by the '399 Patent.

34. Upon information and belief, Defendants have jointly infringed the '399 Patent, including by controlling and/or directing others to perform one or more of the claimed method steps.

35. Defendants are thus liable for infringement of the '399 Patent pursuant to 35 U.S.C. § 271.

36. Defendants' aforementioned acts have caused damage to Plano Encryption in the past and will continue to do so in the future.

COUNT TWO

INFRINGEMENT OF U.S. PATENT NO. 5,974,550

37. Plaintiff Plano Encryption realleges and incorporates herein the preceding paragraphs of its Complaint.

38. Defendants have directly infringed and continue to infringe at least claim 14 of the '550 Patent by making, using, testing, selling, licensing, offering for sale within the United States at least the Accused Products.

39. On information and belief, Defendants have directly infringed and continue to infringe at least claim 14 of the '550 Patent by making, using, testing, selling, licensing, offering for sale within the United States the Accused Products.

40. On information and belief, Q2's Accused Products are made available for distribution and use through the Apple iOS App Store and the Google Android Play Store and are intended for download onto user mobile devices. Once downloaded onto a mobile device, the mobile application software (which comprises a first process) is authenticated in one address space which operates in an address space different from that of the second process (which operates on remote servers).

41. The mobile devices are intended for download onto mobile devices with iOS and Android-compatible operating systems, where the mobile device must have a processing unit for executing programming instructions storage medium and a local storage media which stores instructions to be executed by the mobile device processor for receiving downloads.

42. On information and belief, instructions at the mobile device are executed to download the Q2 mobile application. The Q2 mobile application comprises a tamper resistant module for use with the particular operating system, which is tamper resistant at least in part because it is code signed, as described above.

43. Further, the mobile app recovers a secret (in particular, at least the SSL/TLS premaster secret described above) only when the integrity of the first process is verified. This secret is used in secure communication between the first and second process, including typical challenge-response protocols such as the entering of a password by the user. On information and belief, the Accused Products use a challenge to determine knowledge by the user that would be otherwise hard to guess. It can be a "security question" (such as a grandmother's maiden name) or a PIN code or other information sent by (for example) an email or text to a mobile phone. The Accused Products receive challenges, encode the challenges using the secret to produce a response, and send the response to the second process running at the server either hosted by Q2 or by Q2's customers, using a session key that is derived from the secret.

44. In the alternative, because the manner of use by Q2 differs in no substantial way from language of the claims, if Q2 is not found to literally infringe, Q2 infringes under the doctrine of equivalents. Defendants' infringement is and has been willful, deliberate and intentional. On information and belief, Defendants had pre-suit knowledge of the '550 Patent no later than May or June 2015. Q2 has acted and continues to act in disregard of the high

likelihood that its actions constitute direct and indirect infringement of a valid patent, and knew or should have known of that objectively high risk.

45. Defendants have knowingly induced and continue to induce users of mobile devices to infringe the '550 Patent, including by intentionally developing, making, marketing, advertising, providing, distributing and licensing the software, documentation, materials, training or support and aiding, abetting, encouraging, promoting or inviting use thereof.

46. Defendants have contributed and continue to contribute to the infringement of the '550 Patent by users of the mobile computing devices, including for example, mobile phones and tablet computers, who use, test, sell, license, offer for sale, distribute and license within the United States, the Accused Products on such devices, by providing the necessary software and related documentation, materials, marketing and advertising, training or support. For example, the above described necessary features of the Accused Products are material components of the patented apparatus as disclosed by the '550 Patent.

47. Upon information and belief, Defendants have jointly infringed the '550 Patent, including by controlling and/or directing others to perform one or more of the claimed method steps.

48. Defendants are thus liable for infringement of the '550 Patent pursuant to 35 U.S.C. § 271.

49. Defendants' aforementioned acts have caused damage to Plano Encryption in the past and will continue to do so in the future.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter judgment and provide relief as follows:

50. That Q2 has directly infringed the Patents-in-Suit literally and/or under the doctrine of equivalents;

51. That Q2 has induced infringement of the Patents-in-Suit;

52. That Q2 has contributed to the infringement of the Patents-in-Suit;

53. That Q2 has willfully infringed the Patents-in-Suit;

54. That Q2 be ordered to account for and pay to Plano Encryption past and future damages, costs, expenses, together with prejudgment and post-judgment interest to compensate for Defendants' infringement of the Patents-in-Suit as provided under 35 U.S.C. § 284, and increase such award by up to three times the amount found or assessed in accordance with 35 U.S.C. § 284, and further including an accounting for infringing sales not presented at trial and an award by the Court of additional damages for any such infringing sales;

55. An award to Plaintiff for enhanced damages resulting from the knowing, deliberate, and willful nature of Defendants' prohibited conduct with notice being made at least as early as the date of the filing of this Complaint, as provided under 35 U.S.C. § 284;

56. That this case be declared exceptional and Plano Encryption be awarded its costs, expenses, and reasonable attorneys' fees in this action pursuant to 35 U.S.C. § 285; and

57. That Plaintiff Plano Encryption be awarded such other equitable or legal relief as this Court deems just and proper under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

Respectfully Submitted,

PLANO ENCRYPTION TECHNOLOGIES, LLC

Dated: July 18, 2016

By: /s/ Jeremy S. Pitcock_*by permission E. DeRieux*__

Jeremy S. Pitcock
Admitted to the Eastern District of Texas
PITCOCK LAW GROUP
1501 Broadway, 12th Floor
New York, NY 10036
(646) 571-2237
(646) 571-2001 Fax
jpitcock@pitcocklawgroup.com

Elizabeth L. DeRieux
State Bar No. 05770585
Capshaw DeRieux, LLP
114 E. Commerce Ave.
Gladewater, TX 75647
Telephone: (903) 845-5770
Email: ederieux@capshawlaw.com

ATTORNEYS FOR PLAINTIFF PLANO ENCRYPTION TECHNOLOGIES, LLC